

TrustedCore V6.0



We make sure



Sie haben...

... technische Fragen oder Probleme?

Wenden Sie sich bitte an unseren Help Desk (siehe Garantieheft).

Aktuelle Informationen zu unseren Produkten, Tipps, Updates usw. finden Sie im Internet: ["www.fujitsu-siemens.com/support"](http://www.fujitsu-siemens.com/support)

Dieses Handbuch wurde erstellt von Xerox Global Services

Herausgegeben von Fujitsu Siemens Computers GmbH

AG 06/07

Ausgabe 1

Bestell-Nr. A26361-D2400-Z120-1-19



TrustedCore V6.0

Beschreibung

Einleitung	1
Bedienung des BIOS-Setup	3
Main Menu – Systemfunktionen	7
Advanced Menu – Erweiterte Systemkonfiguration	14
Security Menu - Sicherheitsfunktionen	22
Power Menu – Energiesparfunktionen	44
Boot Menu – Systemstart	47
Exit Menu – BIOS-Setup beenden	48
Stichwörter	49

Intel und Pentium sind eingetragene Warenzeichen und MMX und OverDrive sind Warenzeichen der Intel Corporation, USA.

Microsoft, MS, MS-DOS und Windows sind eingetragene Warenzeichen der Microsoft Corporation.

Beispiele für Windows-Betriebssysteme: Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP, Windows Vista.

PS/2 und OS/2 Warp sind eingetragene Warenzeichen von International Business Machines, Inc.

Alle weiteren genannten Warenzeichen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber und werden als geschützt anerkannt.

Copyright © Fujitsu Siemens Computers GmbH 2007

Alle Rechte vorbehalten, insbesondere (auch auszugsweise) die der Übersetzung, des Nachdrucks, der Wiedergabe durch Kopieren oder ähnliche Verfahren.

Zuwendungen verpflichten zu Schadenersatz.

Alle Rechte vorbehalten, insbesondere für den Fall der Patenterteilung oder GM-Eintragung. Liefermöglichkeiten und technische Änderungen vorbehalten.

Inhalt

Einleitung	1
Darstellungsmittel	2
Bedienung des BIOS-Setup	3
BIOS-Setup aufrufen	3
Wenn Sie auf Ihrer Festplatte die Phoenix cME FirstWare installiert haben und die Console aufrufen möchten	3
Wenn Sie sofort das "Boot Menu" aufrufen möchten	4
BIOS-Setup mit fehlerhaften Einstellungen	4
BIOS-Setup bedienen	6
BIOS-Setup beenden	6
Main Menu – Systemfunktionen	7
System Date / System Time - Datum / Uhrzeit	7
Diskette A - Diskettenlaufwerk	7
SATA Port	8
Total Sectors	8
Maximum Capacity – Festplattenkapazität	9
Multi – Sector Transfers	9
LBA Mode Control	10
32 Bit I/O Busbreite für Datenübertragung	10
Transfer Mode	10
Ultra DMA Mode – Übertragungsgeschwindigkeit	10
SMART Monitoring	10
Firmware	11
Silent Mode – Geräuschverhalten von Festplatten und optischem Laufwerk	11
Password Status – Status des Festplattenpasswortes anzeigen	12
Boot Features – Systemstart	12
POST Errors – System anhalten	13
Post Diagnostic Screen – Startinformation oder Boot-Logo	13
Boot Menu – Systemstart	13
System Memory – Arbeitsspeicher	13
Extended Memory – Erweiterungsspeicher	13
Advanced Menu – Erweiterte Systemkonfiguration	14
Peripheral Configuration – Schnittstellen und Controller	14
Serial 1 / Serial 2 – Serielle Schnittstellen	15
Serial 1 / 2 Adress: Basis-I/O-Adresse und IRQ	15
Diskette Controller	15
Base I / O adress – Diskettenlaufwerks-Controller	15
NV SATA Configuration	15
USB Control – USB Host Controller	17
USB BIOS Legacy Support	17
MAC LAN	18
MAC LAN Bridge	18
LAN Remote Boot – Betriebssystem laden über LAN	18
Azalia Codec – Audio Controller	18
Advanced System Configuration – Zusätzliche Systemeinstellungen	19
Frame Buffer Size	19
Onboard Video	19
High Precision Event Timer	19

SMART Device Monitoring	20
Fan Control – Lüfterdrehzahl	20
PC Beep Volume	20
DMI Event Logging	20
Event log validity	20
Event log capacity	21
View DMI event log	21
Event Logging	21
Mark DMI events as read	21
Clear all DMI event logs	21
Security Menu - Sicherheitsfunktionen	22
Passwörter vergeben und aufheben	22
Setup/System-Passwort einstellen	22
Setup/System – Passwort aufheben	24
Setup Password Lock – Auswirkung des Setup-Passworts	24
Set System Password – System-Passwort	24
System Password Lock – Auswirkung des System - Passworts	25
SmartCard SystemLock / SystemLock 2 (optional)	26
Zugriffsrechte der SmartCard	27
SmartCard Benutzergruppen	27
Installieren von SystemLock	28
Erstes System der Benutzergruppe oder Einzelsystem für SystemLock einrichten	29
System zu einer Benutzergruppe hinzufügen	31
Administrator-Funktionen ausführen	33
Remote Freischaltung – F4	35
Einschalten des PC mit SystemLock	36
PIN ändern	36
SystemLock deinstallieren	36
Fehlermeldungen	37
Flash-BIOS-Update	37
Fehlermeldung nach einem Flash-BIOS-Update	39
Flash Memory Recovery Mode	40
DeskFlash	40
TPM (Trusted Platform Module) Configuration	41
TPM Support	41
TPM State	41
TPM Physical Presence operations	42
cME Authentication Level	42
Virus Warning - Viruswarnung	42
ATA Vulnerability Protection	43
Diskette Write – Schreibschutz für Diskettenlaufwerk	43
Flash Write – Schreibschutz für System-BIOS	43
Cabinet Monitoring – Schutz nach Öffnen des Gehäuses	43
Power Menu – Energiesparfunktionen	44
Power On Source – Verwaltung der Einschaltquellen	44
Power On Source: LAN – Einschalten über LAN-Controller	44
Power On Source: Wake Up Timer – Einschalten über Zeit	45
Power Failure Recovery – Systemzustand nach einem Stromausfall	45
USB At Power-off	46
USB Keyboard	46
Boot Menu – Systemstart	47

Boot Priority Order 47
 Excluded from Boot Order 47
Exit Menu – BIOS-Setup beenden 48
 Save Changes & Exit – Speichern und beenden 48
 Discard Changes & Exit – Beenden ohne speichern 48
 Get Default Values – Standardeinträge 48
 Load Previous Values – Vorhergehende Einträge 48
Stichwörter 49

Einleitung

Im *BIOS-Setup* können Sie Systemfunktionen und die Hardware-Konfiguration des Geräts einstellen.

Die geänderten Einstellungen sind wirksam, sobald Sie die Einstellungen abspeichern und das *BIOS-Setup* beenden.

In den einzelnen Menüs des *BIOS-Setup* können Sie Einstellungen in folgenden Bereichen vornehmen:

<i>Main:</i>	Systemfunktionen
<i>Advanced:</i>	Erweiterte Systemkonfiguration
<i>Security:</i>	Sicherheitsfunktionen
<i>Boot:</i>	Konfiguration der Startreihenfolge
<i>Power:</i>	Energiesparfunktionen
<i>Exit:</i>	Speichern und beenden



In den folgenden Kapiteln sind die einzelnen Menüs mit ihren Einstellmöglichkeiten in alphabetischer Reihenfolge beschrieben.

Die Einstellmöglichkeiten hängen von der Hardware-Konfiguration Ihres Geräts ab.

Es kann deshalb vorkommen, dass Menüs oder einige Einstellmöglichkeiten im *BIOS-Setup* Ihres Geräts nicht angeboten werden oder die Lage der Menüs abhängig von der *BIOS-Revision* variiert.

Darstellungsmittel

	kennzeichnet Hinweise, bei deren Nichtbeachtung Ihre Gesundheit, die Funktionsfähigkeit Ihres Geräts oder die Sicherheit Ihrer Daten gefährdet sind. Die Gewährleistung erlischt, wenn Sie durch Nichtbeachtung dieser Hinweise Defekte am Gerät verursachen
	kennzeichnet wichtige Informationen für den sachgerechten Umgang mit dem Gerät
	kennzeichnet einen Arbeitsschritt, den Sie ausführen müssen
	kennzeichnet ein Resultat
Diese Schrift	kennzeichnet Eingaben, die Sie mit der Tastatur in einem Programm-Dialog oder in einer Kommandozeile vornehmen, z. B. Ihr Passwort (Name123) oder einen Befehl, um ein Programm zu starten (start.exe)
Diese Schrift	kennzeichnet Informationen, die von einem Programm am Bildschirm ausgegeben werden, z. B.: Die Installation ist abgeschlossen!
<i>Diese Schrift</i>	kennzeichnet <ul style="list-style-type: none"> • Begriffe und Texte in einer Softwareoberfläche, z. B.: Klicken Sie auf <i>Speichern</i>. • Namen von Programmen oder Dateien, z. B. <i>Windows</i> oder <i>setup.exe</i>.
"Diese Schrift"	kennzeichnet <ul style="list-style-type: none"> • Querverweise auf einen anderen Abschnitt z. B. "Sicherheitshinweise" • Querverweise auf eine externe Quelle, z. B. eine Webadresse: Lesen Sie weiter auf www.fujitsu-siemens.com • Namen von CDs, DVDs sowie Bezeichnungen und Titel von anderen Materialien, z. B.: "CD/DVD Drivers & Utilities" oder Handbuch "Sicherheit"
	kennzeichnet eine Taste auf der Tastatur, z. B.: 
Diese Schrift	kennzeichnet Standardeinstellungen in den BIOS Menüeinstellungen. (z. B. <i>enabled</i>)

Bedienung des BIOS-Setup

BIOS-Setup aufrufen

- ▶ Starten Sie das Gerät neu durch Ein-/Ausschalten.
- ↳ Warten Sie bis die Bildschirmausgabe erscheint.
- ▶ Drücken Sie die Funktionstaste **F2**.
- ▶ Wenn ein Setup-Passwort vergeben ist, müssen Sie nun das Setup-Passwort eingeben und mit der Eingabetaste bestätigen.
- ↳ Am Bildschirm wird das Menü Main des BIOS-Setup angezeigt.
- ▶ Drücken Sie die Funktionstaste **F1**.
- ↳ Die BIOS Release Information wird angezeigt:
 - Die Version des BIOS-Setup (z.B. 6.0)
 - Der Ausgabestand (Revision) des BIOS-Setup (z.B. Rev. 1.03.2451)
Dabei geben die letzten Ziffern die Nummer des Mainboards an.
Anhand der Nummer des Mainboards können Sie auf CD "Drivers & Utilities" oder "ServerStart" das entsprechende Technische Handbuch zum Mainboard finden oder Sie können im Internet die entsprechende BIOS-Update Datei laden (siehe ["Flash-BIOS-Update"](#), Seite 37).

Wenn Sie auf Ihrer Festplatte die Phoenix cME FirstWare installiert haben und die Console aufrufen möchten

- ▶ Drücken Sie die Funktionstaste **F4**.
- ↳ Am Bildschirm wird die *Phoenix cME Console* angezeigt.



Diese Funktion können Sie nutzen, wenn Sie auf Ihrer Festplatte die Phoenix cME FirstWare installiert haben.

- ▶ Klicken Sie doppelt auf das Symbol *System Setup*.
- ↳ Das *BIOS-Setup* wird gestartet.

Wenn Sie sofort das "Boot Menu" aufrufen möchten



Diese Funktion können Sie nutzen, wenn Sie Ihr System nicht von dem Laufwerk starten möchten, das im Eintrag *Boot Sequence* im Untermenü *Boot Options* als erste Einstellung angegeben ist.

- ▶ Drücken Sie die Funktionstaste **F12**.
- ↳ Am Bildschirm wird das *Boot Menu* als Popup-Fenster angezeigt. Sie können nun auswählen, von welchem Laufwerk Sie das Betriebssystem starten möchten. Die Auswahlmöglichkeiten sind mit den möglichen Einstellungen im Eintrag *Boot Sequence* im Untermenü *Boot Options* identisch. Ihre Auswahl gilt nur für den aktuellen Systemstart. Beim nächsten Systemstart gelten wieder die Einstellungen im Eintrag *Boot Sequence* im Untermenü *Boot Options*.
- ▶ Wählen Sie mit Hilfe der Cursor-Tasten  oder  aus, von welchem Laufwerk Sie das System jetzt starten möchten und bestätigen Sie die Auswahl mit der Eingabetaste.
- ▶ Falls Sie das BIOS-Setup starten möchten, wählen Sie mit Hilfe der Cursor-Tasten  oder  den Eintrag *Setup* aus und bestätigen Sie die Auswahl mit der Eingabetaste.



Wenn ein Laufwerk mit einem "!" gekennzeichnet ist, dann können Sie dieses Laufwerk nicht zum Booten auswählen. Im *BIOS-Setup* können Sie prüfen, warum dieses Laufwerk nicht zum Booten angeboten wird (im Untermenü von *Boot Options*).

BIOS-Setup mit fehlerhaften Einstellungen

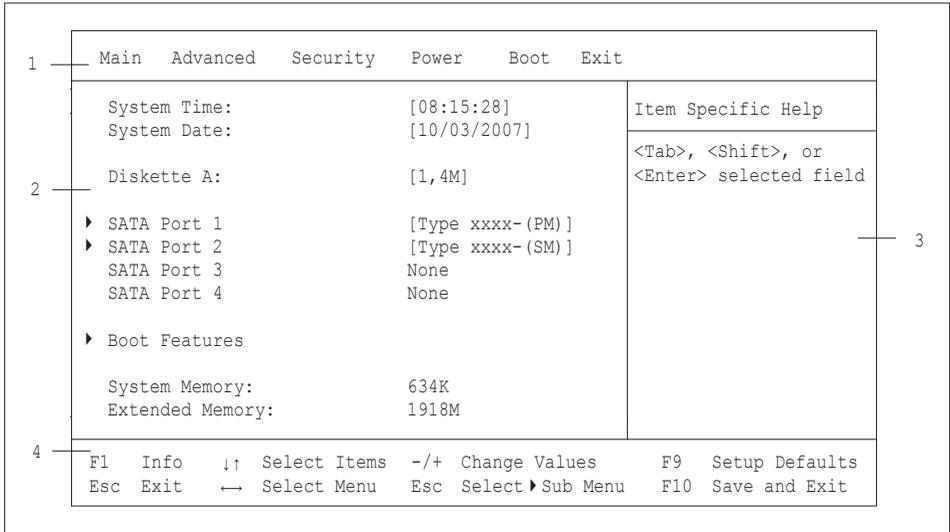


Wenn eine fehlerhafte Einstellung im *BIOS-Setup* den Systemstart verhindert und sich das System dreimal hintereinander nicht starten lässt, werden beim nächsten Systemstart einmalig die Standardeinträge des *BIOS-Setup* eingetragen. Es erscheint die folgende Fehlermeldung:

Previous boot incomplete - Default configuration used

Wenn Sie die Funktionstaste **F2** drücken, können Sie im *BIOS-Setup* die Einstellungen prüfen und korrigieren (siehe Kapitel "[Fehlermeldungen](#)", Seite 37). Wenn eine fehlerhafte Einstellung im *BIOS-Setup* den Systemstart verhindert hat, kann diese jetzt korrigiert werden. Damit ist ein fehlerfreier Systemstart wieder möglich.

Beispiel für das Menü *Main* des *BIOS-Setup*



01 = Menüleiste

03 = Hilfebereich

02 = Arbeitsbereich

04 = Bedienleiste

Der Bildschirm des *BIOS-Setup* ist in folgende Bereiche eingeteilt:

Menüleiste (1): In der Menüleiste können Sie die Menüs des *BIOS-Setup* auswählen.

Arbeitsbereich (2): Im Arbeitsbereich werden die Einstellmöglichkeiten (Felder) des ausgewählten Menüs angezeigt. Die Einträge in den angezeigten Feldern können Sie entsprechend Ihren Anforderungen einstellen.

▶ Kennzeichnet dabei Felder, die weitere Untermenüs öffnen. In diesen Untermenüs können Sie Einträge ändern.

* kennzeichnet dabei Konfigurationskonflikte, die beseitigt werden müssen, um die korrekte Funktion des Geräts zu gewährleisten

Hilfebereich (3): Im Hilfebereich wird eine kurze Information zum ausgewählten Feld angezeigt.

Bedienleiste (4): In der Bedienleiste sind alle Tasten aufgeführt, mit denen Sie das *BIOS-Setup* bedienen können.



Mit der Funktionstaste **F1** können Sie sich zusätzliche Informationen (z. B. BIOS-Version) anzeigen lassen.

BIOS-Setup bedienen

Cursor-Tasten  oder 	Menü aus der Menüleiste auswählen
Cursor-Tasten  oder 	Feld auswählen - das ausgewählte Feld wird hervorgehoben dargestellt
 oder 	Untermenü (mit  gekennzeichnet) öffnen  und beenden 
Tasten  oder  (numerisches Tastaturfeld)	Eintrag für Feld ändern
Funktionstaste 	Standardeinträge für alle Menüs einstellen
Funktionstaste 	Einträge einstellen, die beim Aufruf des <i>BIOS-Setup</i> gültig waren

BIOS-Setup beenden

- ▶ Wählen Sie das Menü *Exit* aus der Menüleiste um das *BIOS-Setup* zu beenden.
- ↳ Sie können dann entscheiden, ob Sie die geänderten Einstellungen speichern wollen.
- ▶ Wählen Sie die gewünschte Möglichkeit.
- ▶ Drücken Sie die Eingabetaste.

Main Menu – Systemfunktionen

Main		Item Specific Help
System Time:	[08:15:28]	<Tab>, <Shift>, or <Enter> selected field
System Date:	[10/03/2007]	
Diskette A:	[1,4M]	
▶ SATA Port 1	[Type xxxx-(PM)]	
▶ SATA Port 2	[Type xxxx-(SM)]	
SATA Port 3	None	
SATA Port 4	None	
▶ Boot Features		
System Memory:	634K	
Extended Memory:	1918M	

Beispiel für das Menu *Main*

System Date / System Time - Datum / Uhrzeit

zeigt das aktuell eingestellte Datum / die aktuell eingestellte Uhrzeit des Geräts an. Das Datum hat das Format "Monat/Tag/Jahr". Die Uhrzeit hat das Format "Stunde/Minute/Sekunde". Wenn Sie das aktuell eingestellte Datum / die aktuell eingestellte Uhrzeit verändern wollen, geben Sie das neue Datum im Feld *System Date* / die neue Uhrzeit im Feld *System Time* ein. Mit der Tabulatortaste können Sie den Cursor innerhalb der Felder *System Time* und *System Date* bewegen.



Wenn die Felder von *System Time* und *System Date* nach dem Aus- und Wiedereinschalten falsche Werte anzeigen, dann ist die Lithium-Batterie leer. Tauschen Sie die Lithium-Batterie aus.

Wie Sie die Lithium-Batterie tauschen ist im Handbuch zum Mainboard beschrieben.

Diskette A - Diskettenlaufwerk

legt den Typ des eingebauten Diskettenlaufwerks fest.

360K, 720K, 1.2M,
1.4M, 2.8M

Der Eintrag hängt vom eingebauten Diskettenlaufwerk ab.

None

Kein Diskettenlaufwerk installiert oder Diskettenlaufwerk wird über IDE Drive oder USB angesprochen.

SATA Port

ruft das Untermenü auf, in dem Sie die Einstellungen für das entsprechende Festplattenlaufwerk vornehmen können. Neben dem jeweiligen Untermenü steht die Herstellerbezeichnung des Laufwerks. Die folgenden Menüpunkte können nicht verändert werden.

SATA Port 1 [Type xxxx-(PM)]		Item Specific Help
Total Sectors:	488397168	HDD Password controls access to the HDD
Maximum Capacity:	250 GByte□	
Multi-Sector Transfers:	[16 Sectors]	
LBA Mode Control:	[Enabled]	
32 Bit I/O:	[Enabled]	
Transfer Mode:	[FPIO 4 / DMA 2]	
Ultra DMA Mode:	[Mode 6]	
Smart Monitoring:	Disabled	
Firmware:	3.AAC	
Password Status:	Not Installed	
Change Password:	[Press Enter]	

Total Sectors

zeigt die Anzahl der Sektoren auf der Festplatte.

Maximum Capacity – Festplattenkapazität

zeigt die Kapazität der Festplatte als LBA-Wert. Der LBA-Wert entspricht der Kapazität, die das BIOS aus der von der Festplatte gemeldeten maximal möglichen Sektorenanzahl errechnet. IDE und BIOS schränken die Einteilung von Festplatten in Zylinder, Köpfe und Sektoren durch maximal zulässige Werte ein. So erlaubt die Festplatte mehr Zylinder, aber weniger Köpfe als das BIOS. Durch die Kombination der Grenzen von IDE und BIOS ergibt sich ein adressierbarer Speicherbereich von höchstens 528 MByte.

Die folgende Tabelle listet die maximal zulässigen Werte und die sich daraus ergebenden maximal nutzbaren Speicherkapazitäten auf.

	BIOS	IDE	Kombination BIOS/IDE
Max. Sektoren pro Kopf (a 512 Byte)	63	255	63
Max. Köpfe pro Zylinder	256	16	16
Max. Zylinder	1024	65535	1024
Kapazität	8,4 GByte	137 GByte	528 MByte

Die LBA Translation rechnet die physikalische Einteilung von Festplatten in Zylinder, Köpfe und Sektoren so um, dass die erzeugten logischen Werte innerhalb der vom BIOS vorgegebenen Grenzen liegen. Auf diese Weise können mehr als 528 MByte Festplattenkapazität genutzt werden. Betriebssystem und Anwenderprogramme arbeiten mit diesen logischen Festplattenwerten. Festplatten mit mehr als 528 MByte werden mit dem LBA-Modus eingerichtet und betrieben. Unterstützt die Festplatte den LBA-Modus, dann ist die volle Speicherkapazität der Festplatte nutzbar.

Das BIOS unterstützt außerdem die 48-Bit-Adressierung für Festplatten. Dieser Industriestandard spezifiziert Festplattenkapazitäten bis zu 144 PByte (Petabyte) - etwa das 120.000-fache der 137-GByte-Grenze.

Multi – Sector Transfers

zeigt die Anzahl der Sektoren pro Block an, die automatisch vom BIOS erkannt werden.

- [0] Disabled
- [1] 2 Sectors
- [2] 4 Sectors
- [3] 8 Sectors
- [4] 16 Sectors**

LBA Mode Control

stellt die Adressierung über fortlaufende Sektornummern (LBA = Logical Block Addressing) ein.

Enabled Wenn die Festplatte den LBA-Modus unterstützt und ihre Speicherkapazität größer als 528 Mbyte ist, dann verwendet das BIOS umgewandelte Festplattenparameter. Dadurch kann die volle Speicherkapazität der Festplatte genutzt werden.

Disabled Das BIOS benutzt die Festplattenparameter und unterstützt damit eine Speicherkapazität bis zu 528 Mbyte.

32 Bit I/O Busbreite für Datenübertragung

legt die Busbreite für die Datenübertragung zwischen Prozessor und Festplatten – Controller fest.

Enabled Die Datenübertragung erfolgt 32-bit-breit am PCI-Bus. Dies steigert die Performance.

Disabled Die Datenübertragung erfolgt 16-bit-breit.

Transfer Mode

legt die Transfermethode fest, um Daten von der Festplatte zum Arbeitsspeicher zu übertragen.

[0] Standard

[1] Fast PIO_1

[2] Fast PIO_2

[3] Fast PIO_3

[4] Fast PIO_4

[5] FPIO 3 / DMA 1

[6] FPIO 4 / DMA 2

Ultra DMA Mode – Übertragungsgeschwindigkeit

legt einen schnellen Ultra-DMA-Übertragungsmodus für das Festplattenlaufwerk fest.

Disabled Der schnelle Ultra-DMA-Übertragungsmodus ist nicht eingestellt.

Mode 0, 1, 2, 3, 4, 5, 6 Ein schneller Ultra-DMA-Übertragungsmodus ist eingestellt.

SMART Monitoring

zeigt an, ob SMART (Self Monitoring Analysis Reporting Technology) Monitoring (Selbstüberwachung, Analyse und Statusmeldung) für die Festplatte aktiviert ist.

Enabled SMART Monitoring ist eingeschaltet.

Disabled SMART Monitoring ist ausgeschaltet.

Firmware

zeigt die Firmware-Versionsnummer des Festplatten-Controllers an.

Silent Mode – Geräuschverhalten von Festplatten und optischem Laufwerk

legt das Geräuschverhalten von Festplatte oder optischem Laufwerk fest. Um den Geräuschpegel des Laufwerks zu senken, wird die Umdrehungsgeschwindigkeit verringert. Das Laufwerk muss diese Funktion unterstützen.

- Disabled** Das Laufwerk arbeitet mit seiner höchsten Umdrehungsgeschwindigkeit.
- Medium* Abhängig vom Laufwerk wird die Umdrehungsgeschwindigkeit auf einen mittleren Wert verringert. Das Laufwerk erzeugt im Betrieb weniger Geräusche und die Performance reduziert sich geringfügig.
- Silent* Abhängig vom Laufwerk wird die Umdrehungsgeschwindigkeit auf den niedrigsten Wert verringert. Das Laufwerk erzeugt im Betrieb weniger Geräusche und die Performance reduziert sich.

Password Status – Status des Festplattenpasswortes anzeigen

zeigt an, in welchem Sicherheitszustand sich die Festplatte befindet.

Not Supported	Die Festplatte unterstützt kein Passwort. Für diese Festplatte können Sie kein Passwort vergeben.
<i>Not Installed</i>	Es ist kein Passwort für die Festplatte vergeben.
<i>Installed</i>	Ein Passwort für die Festplatte wurde gerade vergeben.
<i>Count expired</i>	Die maximale Anzahl der zulässigen Eingabeversuche ist überschritten. Schalten Sie das System aus und versuchen Sie es erneut.
<i>Locked</i>	Die Festplatte ist geschützt und für den Zugriff muss ein Passwort eingegeben werden.
<i>DCO (Power Cycle)</i>	DCO (Device Configuration Overlays) ist gesperrt. Schalten Sie das System aus und versuchen Sie es erneut.
<i>Frozen until Power off</i>	Um den Sicherheitszustand der Festplatte zu ändern, schalten Sie das System aus und wieder ein. Rufen Sie beim Starten des Systems das BIOS-Setup auf und nehmen Sie die gewünschten Einstellungen vor.
<i>Change Password</i>	Das Festplattenpasswort schützt Sie vor unerlaubtem Zugriff auf Ihre Festplattenlaufwerke. Nur die Person, die das Festplattenpasswort kennt, kann das Betriebssystem booten oder Daten auf der Festplatte abrufen. Das Passwort muss vier bis acht Zeichen lang sein. Es dürfen alle alphanumerischen Zeichen verwendet werden, zwischen Groß- und Kleinschreibung wird nicht unterschieden. Passwörter werden bei der Eingabe nicht angezeigt. Die Einstellungen sind umgehend aktiv und bleiben aktiv, unabhängig von der Art, in der das BIOS Setup beendet wird. Der Status des Festplattenpassworts wird gemäß der aktuellen Einstellungen angezeigt (<i>Installed/Not Installed</i>).
<i>Hard Disk Master Password</i>	Der Zugriff auf die Festplatte wird auch durch die Eingabe des Master Passworts gewährt. Dies ist für Situationen gedacht, in denen das normale Passwort vergessen oder unbekannt ist. Das Master Passwort wird geheim gehalten und kann beim Fujitsu Siemens Kundendienst angefragt werden. Das Master Passwort kann deaktiviert werden, so dass der Zugriff auf die Festplatte einzig mit dem normalen Passwort möglich ist.

Boot Features – Systemstart

ruft das Untermenü auf, in dem Sie die Einstellungen für den Systemstart des Geräts vornehmen können.

Boot Features		Item Specific Help
POST Errors:	[Enabled]	Pauses and displays SETUP entry or resume boot prompt if error occurs on boot. If disabled, system always attempts to boot
POST Diagnose Screen:	[Disabled]	
Boot Menu:	[Enabled]	

POST Errors – System anhalten

legt fest, ob der Systemstart nach einem erkannten Fehler abgebrochen wird und das System anhält.

Enabled Wenn der Selbsttest einen Fehler erkennt, wird nach dem Selbsttest der Systemstart abgebrochen und das System angehalten.

Disabled Der Systemstart wird nicht abgebrochen. Der Fehler wird ignoriert - sofern möglich.

Post Diagnostic Screen – Startinformation oder Boot-Logo

Am Bildschirm wird die Startinformation anstatt des Boot-Logos angezeigt.

Enabled Die Startinformationen werden am Bildschirm angezeigt.

Disabled Das Logo wird angezeigt. Bei auftretenden Fehlern oder wenn Sie die Taste drücken, wird auf die Startinformationen umgeschaltet.

Boot Menu – Systemstart

legt fest, ob während des POST mit der Taste das Boot-Menü aufgerufen werden kann.

Enabled Das Menü *Boot* kann aufgerufen werden.

Disabled Das Menü *Boot* kann nicht aufgerufen werden.

System Memory – Arbeitsspeicher

zeigt die Größe des verfügbaren Arbeitsspeichers unterhalb von 1 Mbyte.

Extended Memory – Erweiterungsspeicher

zeigt die Größe des Hauptspeichers an, der oberhalb von 1 Mbyte liegt.

Advanced Menu – Erweiterte Systemkonfiguration



Ändern Sie die Standardeinstellungen nur bei Spezialanwendungen. Falsche Einstellungen können zu Fehlfunktionen führen.

Advanced	
<p style="text-align: center;">Setup Warning</p> <p>Setting items on this menu to incorrect values may cause your system to malfunction.</p> <ul style="list-style-type: none"> ▶ Peripheral Configuration ▶ Advanced System Configuration ▶ DMI Event Logging 	<p>Item Specific Help</p> <hr/> <p>Peripheral Configuration</p>

Beispiel für das Menü *Advanced*

Peripheral Configuration – Schnittstellen und Controller

ruft das Untermenü auf, in dem Sie die Schnittstellen und Controller einstellen können.

Peripheral Configuration	
<p>Serial 1: [Auto]</p> <p>Diskette Controller: [Enabled] Base I/O address: [Primary]</p> <ul style="list-style-type: none"> ▶ NV SATA Configuration <p>USB Control [USB1.1+USB2] USB BIOS Legacy Support [Enabled]</p> <p>MAC LAN: [Enabled] MAC LAN Bridge: [Auto] LAN Remote Boot: [Enabled]</p>	<p>Item Specific Help</p> <hr/> <p>Configure serial port using options</p> <p>[Disabled] No configure</p> <p>[Enabled] User configuration</p> <p>[Auto] BIOS or OS chooses configuration</p>

Beispiel für das Menü *Peripheral Configuration*

Serial 1 / Serial 2 – Serielle Schnittstellen

stellt die Adresse und den Interrupt der entsprechenden seriellen Schnittstelle ein.

Enabled Die serielle Schnittstelle ist auf die angezeigte Adresse und auf den angezeigten Interrupt eingestellt. Wenn Sie Enabled einstellen, erscheinen weitere Zeilen zum Einstellen der Konfiguration. Die serielle Schnittstelle stellt sich automatisch auf eine verfügbare Kombination (Adresse, Interrupt) ein.

Disabled Die serielle Schnittstelle ist ausgeschaltet.

Auto Die serielle Schnittstelle wird automatisch vom BIOS oder vom Betriebssystem ausgewählt.

Serial 1 / 2 Address: Basis-I/O-Adresse und IRQ

legt die Basis-I/O-Adresse und den Interrupt für die serielle Schnittstelle fest.

3F8h/IRQ4, *2F8h/IRQ3*, *3E8h/IRQ4*, *2E8h/IRQ3*

Die serielle Schnittstelle benutzt die ausgewählte Adresse und den ausgewählten Interrupt.

Diskette Controller

Schaltet den Diskettenlaufwerks-Controller des Mainboards ein oder aus.

Enabled Der Diskettenlaufwerks-Controller ist eingeschaltet - IRQ6 ist belegt.

Disabled Der Diskettenlaufwerks-Controller ist ausgeschaltet - IRQ6 ist verfügbar.

Base I / O adress – Diskettenlaufwerks-Controller

ermöglicht die Konfiguration, wenn mehr als ein Diskettenlaufwerks-Controller vorhanden ist.

Primary Standard Basis-I/O-Adresse für den Diskettenlaufwerks-Controller auf dem Mainboard.

Secondary Ermöglicht die Verwendung eines zusätzlichen, externen Diskettenlaufwerks-Controllers.

NV SATA Configuration

ruft das Untermenü zur Konfiguration der/des SATA-Controller auf.

► Aktivieren Sie die SATA Controller, um Einstellungen vorzunehmen.



Damit die Einstellungen wirksam werden, ist u.U. ein Neustart des Systems notwendig

SATA0 Controller

ermöglicht den ersten SATA-Controller ein und aus zu schalten.

Enabled Der erste SATA-Controller ist eingeschaltet. An diesem SATA-Controller angeschlossene Geräte können verwendet werden.

Disabled Der erste SATA-Controller ist ausgeschaltet. An diesem SATA-Controller angeschlossene Geräte können nicht benutzt werden.

SATA0 Mode

legt fest, in welchem Betriebsmodus die SATA-Schnittstellen benutzt werden. Der SATA Modus kann nur angepasst werden, wenn die RAID Funktionalität inaktiv ist.

Native wird von den meisten Betriebssystemen verwendet.

Compatible Der Controller verwendet ausschließlich die Standard Legacy-Resources IRQs 14/15 und I/O 1F0h/1F7h.

SATA1 Controller

ermöglicht den zweiten SATA-Controller ein und aus zu schalten.

Enabled Der zweite SATA-Controller ist eingeschaltet. An diesem SATA-Controller angeschlossene Geräte können verwendet werden.

Disabled Der zweite SATA-Controller ist ausgeschaltet. An diesem SATA-Controller angeschlossene Geräte können nicht benutzt werden.

NV RAID Configuration

Das Mainboard muss die Funktion unterstützen. Die SATA-Schnittstellen werden als RAID System verwendet. Zwei identische serielle ATA-Festplattenlaufwerke müssen angeschlossen sein.

Zusätzliche Einstellungen werden in dem RAID Menü *Utility* vorgenommen. Dieses *Utility* kann beim Booten des Systems mit der Taste **F10** gestartet werden. Auf dem Bildschirm erscheint hierzu eine Meldung.

Enabled Die RAID Funktion ist eingeschaltet und kann im BIOS Setup und im RAID Configuration Menu konfiguriert werden.

Disabled Die RAID Funktion ist ausgeschaltet.

Master SATA0 Primary (SATA Port 1)

legt fest, ob ein ATA-Laufwerk für RAID verfügbar ist.

Enabled ATA-Laufwerk ist verfügbar für RAID.

Disabled ATA-Laufwerk ist nicht verfügbar für RAID.

Master SATA0 Secondary (SATA Port 2)

legt fest, ob ein ATA-Laufwerk für RAID verfügbar ist.

Enabled ATA-Laufwerk ist verfügbar für RAID.

Disabled ATA-Laufwerk ist nicht verfügbar für RAID.

Master SATA1 Primary (SATA Port 3)

legt fest, ob ein ATA-Laufwerk für RAID verfügbar ist.

Enabled ATA-Laufwerk ist verfügbar für RAID.

Disabled ATA-Laufwerk ist nicht verfügbar für RAID.

Master SATA1 Secondary (SATA Port 4)

legt fest, ob ein ATA-Laufwerk für RAID verfügbar ist.

Enabled ATA-Laufwerk ist verfügbar für RAID.

Disabled ATA-Laufwerk ist nicht verfügbar für RAID.

USB Control – USB Host Controller

legt fest, ob der USB-Controller eingeschaltet oder ausgeschaltet (*Disabled*) wird. Ist diese Funktion ausgeschaltet, wird der USB-Controller von keinem Betriebssystem erkannt. Somit können keine USB-Geräte betrieben werden.

[0] Disabled

[1] USB 1.1

[2] **USB 1.1 + USB 2.0**

USB BIOS Legacy Support

legt fest, ob die USB-Tastatur-Emulation auch nach dem Start des Betriebssystems noch aktiv ist. Bei vorhandener USB-Tastatur ist die Emulation für das BIOS-Setup immer eingeschaltet. Weiterhin wird diese Funktion benötigt, wenn man das Betriebssystem von einem USB-Gerät starten möchte.

Enabled Die Funktion ist eingeschaltet. Die USB-Tastatur/-Maus können auch unter Betriebssystemen verwendet werden, wenn diese USB nicht unterstützen. Das Betriebssystem kann von einem USB-Gerät aus gestartet werden, wenn das Betriebssystem dies ebenfalls unterstützt.

Disabled Die Funktion ist ausgeschaltet. Um eine USB-Tastatur/-Maus betreiben zu können, muss diese vom Betriebssystem unterstützt werden. Das Betriebssystem kann nicht von einem USB-Gerät gestartet werden.



Die Funktion *USB BIOS Legacy Support* sollte ausgeschaltet (*Disabled*) sein, wenn das Betriebssystem USB unterstützt und Sie das Betriebssystem nicht von USB-Geräten starten möchten.

MAC LAN

Legt fest, ob der LAN-Controller auf dem Mainboard verfügbar ist.

- Enabled** Onboard LAN-Controller ist aktiviert.
- Disabled* Onboard LAN-Controller ist nicht aktiviert.

MAC LAN Bridge

Das integrierte LAN unterstützt zwei verschiedene Modi: Bridge Mode und MAC Mode.

- Enabled* LAN-Controller ist als Standard LAN-Gerät konfiguriert.
- Disabled* LAN-Controller ist als Bridge-Gerät konfiguriert.
- Auto** LAN-Controller ist automatisch konfiguriert.

LAN Remote Boot – Betriebssystem laden über LAN

ermöglicht das Laden des Betriebssystems von einem Server. Diese Funktion wird besonders dann benutzt, wenn weder Disketten- noch Festplattenlaufwerke vorhanden sind oder diese abgeschaltet wurden. Dabei gibt es zwei verschiedene Systemstart-Protokolle:

- Enabled** Das LAN-BIOS wird aktiviert und ermöglicht es, das Betriebssystem über eine lokale Netzwerkverbindung mit von einem Server zu laden.
- Disabled* Das LAN-BIOS ist deaktiviert.

Azalia Codec – Audio Controller

ermöglicht den Audio-Controller des Mainboards abzuschalten.

- Enabled** Der onboard Audio-Controller ist eingeschaltet.
- Disabled* Der onboard Audio-Controller ist ausgeschaltet.

Advanced System Configuration – Zusätzliche Systemeinstellungen

Advanced System Configuration		
Frame Buffer Size:	[128M]	Item Specific Help
Onboard Videos	[Disablbd]	
High Precision Event Timer:	[Enabled]	Enter frame buffer size for NVIDIA integrated grafic
SMART Device Monitoring:	[Disabled]	
Fan Control:	[Disabled]	
PC Beep Volume:	[Low]	

Beispiel für das Menü *Advanced System Configuration*

ruft das Untermenü auf, in dem Sie zusätzliche Systemeinstellungen vornehmen können.

Frame Buffer Size

hier können Sie die Größe des intern genutzen Grafikspeichers festlegen.

[0] 16M

[1] 32M

[2] 64M

[3] **128M**

Onboard Video

Sie können den Grafikkontroller auf dem Mainboard ausschalten, wenn Sie in dem PC eine Grafikkarte einbauen.

Enabled Grafikkontroller auf dem Mainboard ist eingeschaltet.

Disabled Grafikkontroller auf dem Mainboard ist ausgeschaltet.

High Precision Event Timer

Um den Anforderungen von zeitkritischen Applikationen zu genügen, kann das Betriebssystem den High Precision Event Timer verwenden, wenn dieser aktiviert ist. Dieser erweiterte Timer wird auch Multimedia Timer genannt.

Enabled Der High Precision Event Timer ist eingeschaltet.

Disabled Der High Precision Event Timer ist ausgeschaltet.

SMART Device Monitoring

Sie können SMART (Self Monitoring Analysis Reporting Technology) ein- und ausschalten. SMART kann verwendet werden, um Festplatten-Fehlfunktionen vorherzusagen.

Enabled SMART ist eingeschaltet.

Disabled SMART ist ausgeschaltet.

Fan Control – Lüfterdrehzahl

schaltet die automatische Lüftersteuerung ein und aus. Sie ist dann abhängig vom Temperatursensor.

Enabled Fan Control ist eingeschaltet.

Disabled Fan Control ist ausgeschaltet.

PC Beep Volume

hier kann die Lautstärke des PC-Beeptons eingestellt werden.

High die Lautstärke des Beeptons erhöhen.

Low die Lautstärke des Beeptons verringern.

Off den Beeptons ausschalten.

DMI Event Logging

DMI Event Logging		Item Specific Help
Event log validity	Valid	View the contents of the DMI event log.
Event log capacity	Space Available	
View DMI event log	[Enter]	
Event Logging	[Enabled]	
Mark DMI events as read	[Enter]	
Clear all DMI event logs	[No]	

Das Menü *DMI Event Logging* bietet Ihnen die Möglichkeit, das BIOS Event Log zu betrachten, zu löschen und zu verwalten.

Event log validity

zeigt an, ob die Event Log Einträge gültig sind.

Event log capacity

zeigt an, ob Speicherplatz für neue Event Log Einträge vorhanden ist.

Space Available Es ist noch Platz für weitere Einträge vorhanden.
Full Der Event Log Speicher ist voll.

View DMI event log

► Drücken Sie die Eingabetaste, um alle verfügbaren DMI Event Log Einträge anzuzeigen.

Event Logging

ermöglicht das Aktivieren und Deaktivieren des DMI Event Loggings.

Enable Event Logging ist eingeschaltet.
Disabled Event Logging ist ausgeschaltet.

Mark DMI events as read

► Drücken Sie die Eingabetaste, um DMI events als gelesen zu markieren.



Informationen, die in das *BIOS-Setup* aufgenommen werden sollen, um in *event log messages* betrachtet zu werden, werden deaktiviert.

Clear all DMI event logs

► Wählen Sie "Yes", um alle DMI Event Logs mit dem nächsten Booten zu löschen.
↳ Nach dem Löschen der DMI Event Logs wird diese Option automatisch auf "No" zurückgesetzt.

No **Standardeinstellung**

Security Menu - Sicherheitsfunktionen

Das Menü *Security* bietet Ihnen verschiedene Möglichkeiten, Ihre persönlichen Daten gegen unbefugten Zugriff zu schützen. Sie können diese Möglichkeiten auch sinnvoll kombinieren, um einen optimalen Schutz Ihres Systems zu erreichen.

Security		Item Specific Help
Setup Password	Not Installed	Setup Password controls access to the setup utility
System Password	Not Installed	
Set Setup Password	[Enter]	
Setup Password Lock:	[Standard]	
Set System Password	[Enter]	
System Password Lock:	[Standard]	
▶ SmartCard SystemLock		
CME Authentication Level	[High]	
Virus Warnung	[Disabled]	
ATA Vulnerability Protection	[Standard]	
Diskette Write:	[Enabled]	
Flash Write:	[Enabled]	

Passwörter vergeben und aufheben

Setup/System-Passwort einstellen

Mit dem Setup-Passwort können Sie das unbefugte Aufrufen des *BIOS-Setup* verhindern. Nur wer das Setup-Passwort kennt, kann das *BIOS-Setup* aufrufen. Mit dem System-Passwort können Sie den unbefugten Zugriff auf Ihrem Gerät verhindern. Sie können mit dem System-Passwort das Starten des Betriebssystems sperren. Nur wer das System-Passwort kennt, kann auf das System zugreifen. Damit das System-Passwort wirksam ist, müssen Sie auch das Setup-Passwort vergeben.



Das Passwort muss vier bis acht Zeichen lang sein. Es dürfen alle alphanumerischen Zeichen verwendet werden, zwischen Groß- und Kleinschreibung wird nicht unterschieden.

Passwörter werden bei der Eingabe nicht angezeigt.

Wenn Sie Ihre Passwörter vergessen haben, wenden Sie sich an unseren technischen Kundendienst.

- ▶ Um das Setup/System-Passwort zu vergeben oder zu ändern, gehen Sie folgendermaßen vor:
- ▶ Rufen Sie das *BIOS-Setup* auf und wählen Sie das Menü *Security*.

- ▶ Markieren Sie das Feld *Set Setup Password* bzw. *Set System Password* und drücken Sie die Eingabetaste.
- ↳ Wenn bereits ein Passwort eingestellt ist, werden Sie aufgefordert dieses einzugeben:
Enter Current Password
Sie werden aufgefordert, das neue Passwort einzugeben:
Confirm New Password
- ▶ Geben Sie das Passwort noch einmal ein und drücken Sie die Eingabetaste.
- ↳ Das neue Passwort wird gespeichert.
Changes have been saved [Continue]
Für das Setup-Passwort:
Sie können nun einstellen, ob Sie mit dem Setup-Passwort das Aufrufen des *BIOS-Setup* oder zusätzlich auch den Zugriff auf die Einstellungen der eingebauten Baugruppen mit eigenem BIOS sperren wollen.
- ▶ Um nur das Aufrufen des *BIOS-Setup* zu sperren, markieren Sie das Feld *Setup Password Lock* und wählen Sie den Eintrag *Standard*.
- ▶ Um zusätzlich zum Aufrufen des *BIOS-Setup* auch den Zugriff auf die Einstellungen der eingebauten Baugruppen mit eigenem BIOS zu sperren, markieren Sie das Feld *Setup Password Lock* und wählen Sie den Eintrag *Extended*.
- ↳ Für das System-Passwort:



Verwenden Sie nicht den Eintrag *Keyboard*, um Tastatur und Maus zu sperren, sondern die Sicherheitsfunktionen Ihres Betriebssystems.

Wenn Sie keine weiteren Einstellungen vornehmen wollen, können Sie das *BIOS-Setup* beenden.

- ▶ Um das Starten des Betriebssystems zu sperren, markieren Sie das Feld *Password Mode* und wählen Sie den Eintrag *System*.
- ▶ Wählen Sie im Menü *Exit* die Möglichkeit *Save Changes & Exit*.
- ↳ Das Gerät startet neu und das neue Setup/System-Passwort ist wirksam.

Setup/System – Passwort aufheben



Wenn Sie das Setup-Passwort aufheben, heben Sie damit auch die Wirksamkeit des System-Passworts auf.

Um das Setup/System-Passwort aufzuheben, ohne ein neues einzustellen:

- ▶ Rufen Sie das *BIOS-Setup* auf und wählen Sie das Menü *Security*.
- ▶ Markieren Sie das Feld *Set Setup Password* bzw. *Set System Password* und drücken Sie die Eingabetaste.
- ↳ Sie werden aufgefordert, das aktuelle Passwort einzugeben:
Current Password
- ▶ Geben Sie das Passwort ein und drücken Sie die Eingabetaste.
- ▶ Drücken Sie weitere zweimal die Eingabetaste.
- ▶ Wählen Sie im Menü *Exit* die Möglichkeit *Save Changes & Exit*.
- ↳ Das Gerät startet neu und das Setup/System-Passwort ist aufgehoben.

Setup Password Lock – Auswirkung des Setup-Passworts

Voraussetzung: Das Setup-Passwort ist installiert.

Das Feld legt die Auswirkung des Setup-Passworts fest (siehe auch ["Passwörter vergeben und aufheben", Seite 22](#)).

Standard

Das Setup-Passwort verhindert das unbefugte Aufrufen des *BIOS-Setup*.

Extended

Das Setup-Passwort verhindert das unbefugte Aufrufen des *BIOS-Setup* und sperrt die Tastatur während der Initialisierungsphase des Geräts. Dadurch wird der unbefugte Zugriff auf Einstellungen von eingebauten Baugruppen mit eigenem BIOS verhindert. Der Zugriff auf das BIOS der Baugruppe ist nur möglich, wenn das Setup-Passwort während der Initialisierung der Baugruppe eingegeben wird. Die Passwort-Eingabe müssen Sie mit der Eingabetaste abschließen. Es erfolgt keine Aufforderung zur Passwortheingabe am Bildschirm.

Set System Password – System-Passwort

Voraussetzung: Das Setup-Passwort ist installiert.

Das Feld ermöglicht die Installation des System-Passworts. Das System-Passwort verhindert den unbefugten Zugriff auf Ihr System.

Wenn Sie das Feld markieren und die Eingabetaste drücken, können Sie das System-Passwort eingeben und bestätigen (siehe auch ["Passwörter vergeben und aufheben", Seite 22](#)).

System Password Lock – Auswirkung des System - Passworts

legt fest, ob das System-Passwort beim Betriebssystemstart über *Wake On LAN* übergangen wird oder eingegeben werden muss.

- | | |
|-----------------|--|
| <i>WOL Skip</i> | Das System-Passwort wird beim Betriebssystemstart über <i>Wake On LAN</i> deaktiviert. |
| <i>Standard</i> | Das System-Passwort muss beim Betriebssystemstart über die Tastatur eingegeben werden. |

SmartCard SystemLock / SystemLock 2 (optional)

SmartCard SystemLock		
SmartCard SystemLock	Not Installed	Item Specific Help
Install Single PC:	[Enter]	Installs the security for this PC, and creates a new SystemLock Admin SmartCard dedicated to this PC.
Install Group PC:	[Enter]	
		SmartCard data will be overwritten.
		A correct SmartCard is required for a permanent installation

Mit *SystemLock* kann der PC nur mit initialisierter SmartCard (SICRYPT, CardOS oder Fujitsu) und persönlicher Geheimnummer (PIN) gestartet werden. SmartCard und PIN werden bereits beim Systemstart im BIOS geprüft, also noch vor dem Betriebssystemstart.



Alle neuen SmartCards haben eine voreingestellte PIN (Personal Identification Number) und PUK (Personal Unblocking Key).

Bei SICRYPT- und CardOS-SmartCards sind PIN und PUK auf *12345678* voreingestellt.

Bei Fujitsu ist die PIN auf *0000* und die PUK auf *administrator* voreingestellt. Aus Sicherheitsgründen sollten Sie PIN und PUK unbedingt ändern.

Damit auch im laufenden Betrieb geprüft wird, ob die richtige SmartCard gesteckt ist, benötigen Sie eine zusätzliche Software wie z. B. Smarty.

Falls Sie im *BIOS-Setup* im Menü *Security* nicht den Eintrag *SmartCard SystemLock* haben, dann unterstützt Ihr System *SystemLock* nicht. Sie können Ihr System-BIOS mit dem *Flash-BIOS-Update* aktualisieren (siehe Kapitel "[Flash-BIOS-Update](#)", Seite 37).



Nachdem Sie die erste SmartCard initialisiert haben, kann im *BIOS-Setup* der Eintrag *SmartCard SystemLock* nicht mehr ausgeschaltet (*Disabled*) werden. Wie Sie *SystemLock* deinstallieren finden Sie unter "[SystemLock deinstallieren](#)", Seite 36.

Zugriffsrechte der SmartCard

Eine neue SmartCard besitzt nur die voreingestellte PIN und PUK. Erst wenn die SmartCard initialisiert wird, werden die Zugriffsrechte festgelegt und die individuelle PIN und PUK vergeben. Je nachdem, welche Zugriffsrechte die SmartCard erhält, wird diese wie folgt bezeichnet:

- User-SmartCard – Starten des Systems, Ändern der PIN
- Super-User-SmartCard – Starten des Systems, Änderungen im *BIOS-Setup*, Ändern der PIN
- Service-SmartCard – Änderungen im *BIOS-Setup*
- Admin-SmartCard – Starten des Systems, Änderungen im *BIOS-Setup*, Ändern der PIN, Deinstallieren von *SystemLock*, Initialisieren von SmartCards, Entsperren von SmartCards

In der folgenden Tabelle finden Sie eine Übersicht, welche Rechte die jeweilige SmartCard bei der Eingabe von PIN oder PUK besitzt:

	User-SmartCard		Super-User-SmartCard		Service-SmartCard		Admin-SmartCard	
	PIN	PUK	PIN	PUK	PIN	PUK	PIN	PUK
System starten	x		x				x	
BIOS-Setup aufrufen			x		x		x	
eigene PIN ändern	x		x		x		x	x
eigene blockierte SmartCard entsperren		x*		x*		x*		x
alle blockierten SmartCards entsperren								x
Benutzerkarten erzeugen								x
SystemLock deinstallieren								x

* Im *BIOS-Setup* eingestellt (*Unblock own SmartCard*)

Üblicherweise gibt es immer eine Admin-SmartCard und mindestens eine User- oder Super-User-SmartCard, um ein System zu bedienen.

SmartCard Benutzergruppen

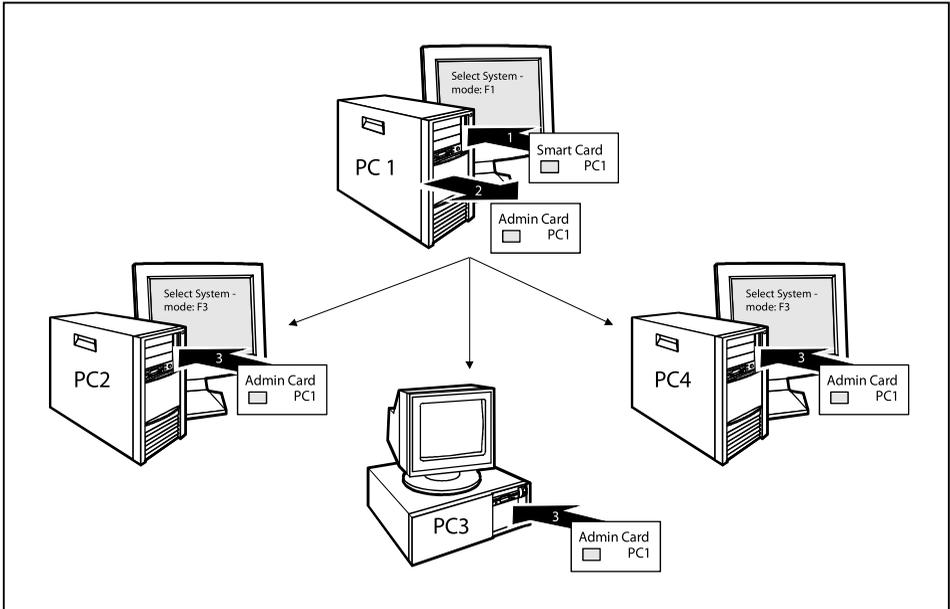
Mit *SystemLock* können Benutzergruppen gebildet werden. Damit ist es möglich, mit einer SmartCard mehrere Systeme zu starten. Eine Benutzergruppe besteht aus mindestens zwei Systemen. Jeder Benutzer, der die Systeme starten darf, erhält eine SmartCard. Mit dieser SmartCard kann der Benutzer wahlweise eines der Systeme starten.

Grundsätzliches zum Einrichten von Benutzergruppen

Bei der Installation von *SystemLock* wird der erste PC in der Benutzergruppe als "Single PC" eingerichtet. Mit der dabei entstehenden Admin-SmartCard wird die Benutzergruppe gebildet. Jeder weitere PC wird bei der Installation von *SystemLock* als "Group PC" eingerichtet. Die vorhandene Admin-SmartCard wird gesteckt, die Informationen werden

eingelassen und der PC wird zur Benutzergruppe hinzugefügt. Die Admin-SmartCard entscheidet, zu welcher Benutzergruppe der PC gehört.

Wenn Sie FSC-CardOS SmartCards verwenden, dann kann *SystemLock* mit dem Windows Programm "SystemLock Admin" administriert werden. Mit "SystemLock Admin" können Sie *SystemLock* komfortabel auf Betriebssystemebene verwalten, *SystemLock* Organisationseinheiten und Gruppen anlegen, SmartCards für die Organisationseinheiten oder Gruppen erzeugen, Zugangsberechtigungen verschiedener Stufen für Userkarten erteilen, sowie Zugangsberechtigungen remote wiederherstellen. Sie können die PIN oder PUK Ihrer SmartCard oder der SmartCards von anderen Benutzern ändern und gesperrte Karten wieder aktivieren. Die genaue Beschreibung entnehmen Sie dem Hilfe-Manual von "SystemLock Admin".



Damit die Benutzer Zugang zu den Systemen innerhalb einer Benutzergruppe erhalten, müssen über *SystemLock* noch User-SmartCards oder Super-User-SmartCards erzeugt werden. Mit einer User-SmartCard oder Super-User-SmartCard kann sich ein Benutzer an jedes System innerhalb der Benutzergruppe anmelden.

Installieren von SystemLock

Beim ersten Installieren wird die erste SmartCard zur Admin-SmartCard. Sie hat zusammen mit der PUK alle Zugriffsrechte und sollte deshalb an einem sicheren Ort aufbewahrt werden. Sie darf nur von einem autorisierten Benutzer (Administrator) verwendet werden, um z. B. Benutzerkarten zu initialisieren.

Wenn Sie eine Benutzergruppe einrichten wollen, benötigen Sie eine Admin-SmartCard. Diese Admin-SmartCard verwenden Sie, um weitere Systeme zur Benutzergruppe hinzuzufügen.

Erstes System der Benutzergruppe oder Einzelsystem für SystemLock einrichten

- ▶ Starten Sie den PC und rufen Sie das BIOS-Setup auf.
- ▶ Wählen Sie im Menü *Security* die Seite *SmartCard SystemLock*.
- ↳ Es erscheint folgendes SmartCard SystemLock Menü:

Security		
SmartCard SystemLock		Item Specific Help
SmartCard SystemLock	Not Installed	Install the security f[or] this PC, and creates a new SystemLock Admin [User] SmartCard dedicated to this PC. SmartCard data will be written. The correct SmartCard is required for a permanent installation.
Install Single PC	[Enter]	
Install Group PC	[Enter]	
Install Single PC		
Enter the PUK: []		
Enter new PIN: []		
Confirm new PIN: []		

- ▶ Stecken Sie eine neue SmartCard in den Leser und drücken Sie die Eingabetaste.



Neue Smartcards haben eine voreingestellte PUK (siehe oben).

Wenn Sie eine bereits initialisierte SmartCard neu initialisieren wollen, müssen Sie die PUK kennen, die dieser SmartCard vergeben wurde.

- ▶ Geben Sie die PUK ein.

↳ Es erscheint:

- *ACCESS DENIED* = Sie haben die falsche PUK eingegeben. Nach sechs Fehlversuchen wird die SmartCard gesperrt und kann nicht mehr benutzt werden.

- ▶ Geben Sie bei der nachfolgenden Meldung eine neue PIN ein.

↳ *Enter new PIN:*

Confirm new PIN:



Für die neue PUK sind vier- bis achtstellige Zahlen zulässig. Wir empfehlen Ihnen aus Sicherheitsgründen, die PUK bei jeder SmartCard zu ändern und eine achtstellige Zahl zu verwenden.

► Geben Sie die neue PIN zur Bestätigung noch einmal ein.

↳ Es erscheint:

- *PIN/PUK do not match* = Sie haben die PIN falsch bestätigt. Sie werden aufgefordert, noch einmal die neue PIN einzugeben und zu bestätigen.

Nach der Bestätigung der neuen PIN warten Sie bitte einige Sekunden: *SystemLock* wird installiert. Bei erfolgreicher Installation erscheint die Meldung:

Setup Notice
Changes have been saved
[Continue]

► Drücken Sie nun die Eingabetaste. Es erscheint das SystemLock Administrationsmenü:

Security		
SmartCard SystemLock		Item Specific Help
SmartCard SystemLock	Installed	Allows to deactivate The smartcard security.
Uninstall:	[Enter]	
BIOS Recovery:	[Allowed]	
SmartCard and Pin	[Always required]	
SmartCard Initialization		ATTENTION: Always check the BIOS password settings after uninstalling SystemLock.
Admin SmartCard	[Enter]	
SuperUser SmartCard:	[Enter]	
User SmartCard:	[Enter]	
Service SmartCard:	[Enter]	
SmartCard Configuration		NOTICE: Reinstalling a SinglePC implies re-initializing all of your smartcards
Change PIN:	[Enter]	
Change PUK:	[Enter]	
Unblock SmartCard:	[Enter]	

► Bevor Sie die neue SmartCard entnehmen, sollten Sie aus Sicherheitsgründen die voreingestellte PUK unbedingt ändern. Wählen Sie hierzu unter *SmartCard Configuration* die Option *Change PUK*, drücken Sie die Eingabetaste und geben Sie eine neue PUK ein.

► Geben Sie zuerst die voreingestellte PUK ein.

↳ *Enter the PUK:*

Neue SmartCards haben eine voreingestellte PUK (siehe oben).

Wenn Sie eine bereits initialisierte SmartCard neu initialisieren wollen, müssen Sie die PUK kennen, die an diese SmartCard vergeben wurde.

- ▶ Geben Sie die PUK ein.
- ↳ Es erscheint:
 - *ACCESS DENIED* = Sie haben die falsche PUK eingegeben. Nach sechs Fehlversuchen wird die SmartCard gesperrt und kann nicht mehr benutzt werden.
- ▶ Geben Sie nachfolgend die neue PUK ein.
- ↳ *Enter new PUK:*
- Confirm new PUK:*



Für die neue PUK sind vier- bis achtstellige Zahlen zulässig. Wir empfehlen Ihnen aus Sicherheitsgründen, die PUK bei jeder SmartCard zu ändern und eine achtstellige Zahl zu verwenden.

- ▶ Geben Sie die neue PUK zur Bestätigung noch einmal ein.
- ↳ Es erscheint:
 - *PIN/PUK do not match* = Sie haben die PUK falsch bestätigt. Sie werden dann aufgefordert, noch einmal die neue PUK einzugeben und zu bestätigen.
- Wie Sie eine weitere SmartCard initialisieren finden Sie im Abschnitt ["Administrator-Funktionen ausführen", Seite 33](#).
- ▶ Wenn Sie keine weitere SmartCard initialisieren wollen, drücken Sie **[Esc]** und entnehmen Sie die Admin-SmartCard. Vermerken Sie auf keinen Fall die PIN oder PUK auf der SmartCard!



Bewahren Sie die SmartCard und PIN/PUK an einem sicheren Ort auf und schützen Sie sie vor unberechtigtem Zugriff.

System zu einer Benutzergruppe hinzufügen

- ▶ Starten Sie den PC.
- ▶ Rufen Sie das *BIOS Setup* auf und wählen Sie im Menü *Security* die Seite *SmartCard SystemLock*.
- ↳ Es erscheint folgendes SmartCard SystemLock Menü:

Security		
SmartCard SystemLock		Item Specific Help
SmartCard SystemLock	Not Installed	Installs the security from a SystemLock Admin SmartCard into this PC without modifying any data on the SmartCard.
Install Single PC	[Enter]	
Install Group PC	[Enter]	
Enter PIN: []		Direct SmartCard is required for a permanent installation.

► Stecken Sie die Admin-SmartCard der Benutzergruppe.

↳ *Enter PIN:*

► Geben Sie die PIN ein.

↳ Es erscheint:

- *ACCESS DENIED* = Sie haben die PIN falsch bestätigt. Sie werden dann aufgefordert, noch einmal die neue PIN einzugeben und zu bestätigen. Nach drei Fehlversuchen wird die SmartCard gesperrt und kann nur mit der PUK wieder aktiviert werden.

Enter the PUK:

► Geben Sie die PUK ein.

↳ Es erscheint:

- *ACCESS DENIED* = Sie haben die falsche PUK eingegeben. Nach sechs Fehlversuchen wird die SmartCard gesperrt und kann nicht mehr benutzt werden.

Nach Eingabe der PIN und PUK warten Sie bitte einige Sekunden: *SystemLock* wird installiert.

Bei erfolgreicher Installation erscheint die Meldung:

Setup Notice
Changes have been saved
[Continue]

Drücken Sie nun die Eingabetaste. Es erscheint das SystemLock Administrationsmenü:

Security		
SmartCard SystemLock		Item Specific Help
SmartCard SystemLock	Installed	Allows to deactivate The smartcard security.
Uninstall:	[Enter]	
BIOS Recovery:	[Allowed]	
SmartCard and Pin	[Always required]	
SmartCard Initialization		ATTENTION: Always check the BIOS password settings after uninstalling SystemLock.
Admin SmartCard	[Enter]	
SuperUser SmartCard:	[Enter]	
User SmartCard:	[Enter]	
Service SmartCard:	[Enter]	NOTICE: Reinstalling a SinglePC implies re-initializing all of your smartcards
SmartCard Configuration		
Change PIN:	[Enter]	
Change PUK:	[Enter]	
Unblock SmartCard:	[Enter]	

Erzeugen Sie für den PC eine Benutzerkarte, wie im Abschnitt ["Administrator-Funktionen ausführen", Seite 33](#) beschrieben.

► Wenn Sie keine weitere SmartCard initialisieren wollen, drücken Sie und entnehmen Sie die Admin-SmartCard.

Administrator-Funktionen ausführen

Wenn Sie einen internen SmartCard-Leser besitzen, dann können Sie den PC auch durch Stecken der SmartCard einschalten. Nach dem Einschalten erscheint die Meldung:

Insert a SmartCard.

- ▶ Stecken Sie die Admin-SmartCard. Sie erhalten folgende Meldung:

↳ *Enter PIN.*

Jetzt können Sie wählen:

F2=Setup, F3=Change PIN

- ▶ Drücken Sie die Funktionstaste **[F2]**, um das BIOS Setup zu erreichen.

- ▶ Wählen Sie im Menü *Security* die Seite *SmartCard SystemLock*.

↳ Es erscheint das SystemLock Administrationsmenü:

Security		Item Specific Help
SmartCard SystemLock		
SmartCard SystemLock	Installed	Allows to deactivate The smartcard security.
Uninstall:	[Enter]	
BIOS Recovery:	[Allowed]	
SmartCard and Pin	[Always required]	ATTENTION: Always check the BIOS password settings after uninstalling SystemLock.
SmartCard Initialization		NOTICE: Reinstalling a SinglePC implies re-initializing all of your smartcards
Admin SmartCard	[Enter]	
SuperUser SmartCard:	[Enter]	
User SmartCard:	[Enter]	
Service SmartCard:	[Enter]	
SmartCard Configuration		
Change PIN:	[Enter]	
Change PUK:	[Enter]	
Unblock SmartCard:	[Enter]	

Die weiteren SmartCards sollten entweder als normale User-SmartCard ("System") oder als erweiterte User-SmartCard ("System and Setup") erstellt werden. Diese haben dann einen eingeschränkten Zugang zum PC (siehe Kapitel "[SystemLock deinstallieren](#)", Seite 36).

- ▶ Wählen Sie die gewünschte Funktion. Sie erhalten folgende Meldung:

↳ *Remove your Admin Card.*



Bewahren Sie die Admin-SmartCard an einem sicheren Ort auf und schützen Sie sie vor unberechtigtem Zugriff.

- ▶ Entnehmen Sie die Admin-SmartCard.

↳ *Insert a SmartCard.*

▶ Stecken Sie die nächste SmartCard und initialisieren sie diese wie gewünscht.

↳ Sie erhalten folgende Meldung:

Remove the SmartCard.



Ändern Sie bei allen weiteren SmartCards immer PIN und PUK. Die PUK einer SmartCard wird benötigt, um eine gesperrte SmartCard mit der Funktion Unblock Smartcard wieder zu aktivieren.

▶ Entnehmen Sie die User-SmartCard und beschriften Sie diese, z. B. mit dem Namen des Benutzers. Vermerken Sie aber auf keinen Fall die PIN auf der SmartCard!

Remote Freischaltung – F4

Voraussetzung:

Der PC wird innerhalb einer Organisationseinheit zentral verwaltet und ist in einer SystemLock-Admin Datenbank registriert. Die zur Gruppeninstallation benutzte SmartCard muss zuvor mit dem Windows-Programm *SystemLock Admin.EXE* initialisiert worden sein (siehe "[SmartCard Benutzergruppen](#)", Seite 27).

Um einem Benutzer remote den Zugriff auf einen PC freizuschalten oder einem Gast oder Servicetechniker einen einmaligen Zugriff zu einem PC remote zu erlauben, geht man wie folgt vor:

- ▶ Starten Sie den PC.
- ↳ Die Meldung Insert a SmartCard erscheint.
- ▶ Drücken Sie die Taste F4
- ↳ Es erscheint die Dialogbox:

SmartCard SystemLock	
Org Unit:	Company Department 1
PC Group:	Group 1
I-CODE 1:	0123456789ABCDEF
I-CODE 2:	0123456789ABCDEF
[Continue]	

Der Benutzer muss nun seinen Administrator oder seine Verwaltungs-Hotline kontaktieren und die angezeigten Daten und Codes durchgeben.

Der Administrator legt dann die Art der einmaligen Zugriffsberechtigung fest:

<i>User access</i>	Der Benutzer kann das System einmalig booten.
<i>Service access</i>	Einmaliger Zugriff auf das BIOS zu Servicezwecken, ohne Zugriff auf die SystemLock Funktionen.
<i>Admin access</i>	Zugriff auf das BIOS und die SystemLock Funktionen, z. B. zum Freischalten des PC bei Verlust der zugehörigen SmartCard.

Abhängig von der Festlegung der Zugangsberechtigung wird ein Freischaltcode erzeugt und dem Benutzer über die Hotline mitgeteilt.

Der Benutzer muss zunächst auf dem freizuschaltenden System die Eingabetaste drücken, die erste Hälfte (Code 1) des Freischaltcodes eingeben und mit der Eingabetaste bestätigen. Es erscheint die Dialogbox zur Eingabe und Bestätigung der zweiten Hälfte (Code 2) des Freischaltcodes. Bei falscher Eingabe kann beliebig oft wiederholt werden.

Wurden alle 32 Zeichen des Freischaltcodes richtig eingegeben, startet der PC mit den durch den Administrator zugeordneten Rechten, als wäre eine entsprechende SmartCard gesteckt.

i

Der Freischaltcode kann nur einmal zum Starten des PC verwendet werden; er verfällt sofort, wenn der PC startet. Wenn Sie den PC ausschalten und erneut ohne Ihre SmartCard starten wollen, müssen Sie die zuvor beschriebene Prozedur jedesmal wiederholen.

Einschalten des PC mit SystemLock

Wenn Sie einen internen SmartCard-Leser besitzen, dann können Sie den PC durch Stecken der SmartCard einschalten. Wenn Sie den PC mit dem Ein-/Ausschalter einschalten, dann erscheint die Meldung:

Insert a SmartCard.

- ▶ Stecken Sie Ihre SmartCard.
- ↳ *Enter PIN:*
- ▶ Geben Sie Ihre PIN ein.
- ↳ Es erscheint:
 - *ACCESS DENIED* = Sie haben die falsche PIN eingegeben. Nach drei Fehlversuchen wird die SmartCard gesperrt und kann nur durch Eingabe der PUK wieder freigeschaltet werden.
- ↳ Abhängig von den Rechten Ihrer SmartCard können Sie, während die Meldung am Bildschirm angezeigt wird, folgende Funktionen auswählen:

F2=Setup, F3=Change PIN

Bei entsprechenden Rechten der SmartCard können Sie mit

– das BIOS-Setup starten.

– die PIN ändern.

Wenn Sie keine Funktion auswählen, startet das System.

BIOS-Setup starten –

Es muss eine SmartCard mit den entsprechenden Rechten gesteckt sein (SuperUser, Service oder Admin).

PIN ändern

Ist bei jeder initialisierten SmartCard möglich.

- ▶ Drücken Sie die Funktionstaste .
- ▶ Geben Sie die alte PIN ein.
- ▶ Geben Sie die neue PIN ein.



Für die neue PIN sind vier- bis achtstellige Zahlen zulässig.

Wir empfehlen Ihnen aus Sicherheitsgründen, die PIN bei jeder SmartCard zu ändern und eine achtstellige Zahl zu verwenden.

- ▶ Bestätigen Sie die neue PIN.

SystemLock deinstallieren

- ▶ Starten Sie den PC.
- ▶ Folgen Sie den Anweisungen, wie im Abschnitt ["Administrator-Funktionen ausführen", Seite 33](#). Wählen Sie "Uninstall" zum Deinstallieren von SystemLock.
- ↳ Sie können anschließend den PC wieder ohne SmartCard betreiben.

Fehlermeldungen

In diesem Kapitel finden Sie die Fehlermeldungen, die von den Mainboards ausgegeben werden.

SystemLock – Fehlermeldungen

In diesem Kapitel finden Sie die Fehlermeldungen, die von dem SmartCard-Leser (Chipkartenleser) ausgegeben werden.

<i>Boot access denied</i>	Die SmartCard hat keine Zugriffsrechte auf das System.
<i>Check your SmartCard</i>	Die SmartCard ist entweder falsch gesteckt oder es ist keine geeignete SystemLock-Smart Card.
<i>SmartCard reader FAILURE</i>	Es ist ein Fehler auf der seriellen Schnittstelle zum SmartCard-Leser (Chipkartenleser) aufgetreten. Erscheint dieser Fehler häufiger muss die Verbindung zwischen SmartCard-Leser und Mainboard überprüft oder der SmartCard-Leser getauscht werden. So lange der Fehler auftritt, ist der Zugriff auf das System gesperrt.
<i>Non authorized SmartCard</i>	Die SmartCard ist auf diesem PC nicht verwendbar. Die SmartCard wurde für einen anderen PC konfiguriert.
<i>SystemLock installation FAILED:</i>	Beim Installieren von <i>SystemLock</i> ist ein Fehler aufgetreten. Schalten Sie den PC nicht aus, sondern legen Sie die "BIOS-Flash-Diskette" ein und versuchen Sie die Installation nochmals.
<i>The SmartCard is blocked.</i>	Sie haben die maximale Anzahl an Fehlversuchen bei der PIN-Eingabe überschritten. Die SmartCard ist gesperrt. Geben Sie die Administrator-PUK ein, um die SmartCard wieder zu aktivieren. Danach müssen Sie eine neue Benutzer-PIN eingeben, um das System neu zu starten.
<i>Enter the PUK:</i>	

Flash-BIOS-Update

Um ein *Flash-BIOS-Update* durchzuführen, laden Sie sich zuerst die entsprechende Datei aus dem Internet.

Unter "www.fujitsu-siemens.com" wählen Sie die gewünschte Sprache (deutsch oder englisch) und dann die Rubrik "Treiber/Handbücher". Danach erreichen Sie mit einem Klick auf "Download/Accessories/Mainboards" die Seite im Internet, auf der Sie nachsehen können, ob für Ihren PC ein Flash-BIOS-Update vorhanden ist.

Sie benötigen eine DOS-Boot-Diskette, auf die die BIOS-Update-Datei gespeichert wird. Die so entstandene Diskette heißt Flash-BIOS-Diskette.



Anstatt der Diskette können Sie auch einen DOS-Boot-Memorystick an eine USB-Schnittstelle anstecken oder mit dem Windows-Programm DeskFlash den BIOS-Update durchführen.



Das BIOS ist im Flash Memory gespeichert. Wenn während des Flash-BIOS-Updates ein Fehler auftritt, ist das BIOS-Setup im Flash Memory zerstört. Sie können das BIOS-Setup dann nur noch über den *Flash Memory Recovery Mode* wiederherstellen. Wenn dies nicht mehr möglich ist, tauschen Sie das Flash Memory aus oder wenden Sie sich an unseren Service.

- Notieren Sie sich die Einstellungen im BIOS-Setup.



Ein Flash-BIOS-Update beeinflusst die BIOS-Setup-Einstellungen normalerweise nicht. Sollten jedoch nach dem Flash-BIOS-Update trotzdem einige Einstellungen verändert sein, dann müssen Sie diese neu konfigurieren.



Das System darf während des Programmiervorgangs weder ausgeschaltet noch zurückgesetzt werden!

Unterbrechen Sie das Flash-BIOS-Update auf gar keinen Fall. Das BIOS-Update wird sonst zerstört.

- Starten Sie das System mit eingelegter Flash-BIOS-Diskette.
- ↳ Das Utility *BIOFLASH.EXE* liest zunächst die BIOS-Update-Datei ein.
Nach automatischer Erkennung des Flash-Memory-Typs beginnt der Programmiervorgang. Dabei wird das alte *BIOS-Setup* gelöscht und mit dem Inhalt der BIOS-Update-Datei überschrieben.
Die Bildschirmmeldungen während des Programmiervorgangs sehen beispielsweise so aus:

```
WARNING:  
SYSTEM MUST NOT BE SWITCHED OFF OR RESET WHILE FLASH PROGRAMMING  
IS IN PROCESS. OTHERWISE THE SYSTEM BIOS WILL BE DESTROYED.
```

```
Flash memory: AMD 29F002T
```

```
Erasing 1.BLOCK (64K) /  
Erasing 2.BLOCK (64K) /  
Erasing 3.BLOCK (64K) /  
Erasing 4.BLOCK (32K) /  
Erasing 5.BLOCK (8K) /
```

```
Programming 1.BLOCK (64K) /  
Programming 2.BLOCK (64K) /  
Programming 3.BLOCK (64K) /  
Programming 4.BLOCK (32K) /  
Programming 5.BLOCK (8K) /
```

```
CMOS Configuration updated.
```

```
Flash memory programmed.
```

Wenn das Flash-BIOS-Update beendet ist, erscheint auf dem Bildschirm folgende Meldung:

```
Flash memory programmed.
```

```
Turn off the system and remove flash deskette from drive!
```

- Schalten Sie den PC aus und entfernen Sie die Flash-BIOS-Diskette aus dem Laufwerk A.
- ↳ Beim nächsten Einschalten startet der PC mit der neuen BIOS-Version.

- ▶ Überprüfen Sie die Einstellungen im BIOS-Setup. Konfigurieren Sie diese gegebenenfalls neu.

Fehlermeldung nach einem Flash-BIOS-Update

Wenn die Meldung

BIOS update for installed CPU failed

erscheint, muss der für den gesteckten Prozessor benötigte Mikrocode noch geladen werden.

Gehen Sie vor wie beschrieben:

- ▶ Starten Sie das System mit eingelegter Flash-BIOS-Diskette.
- ▶ Brechen Sie den normalen Flash-Vorgang ab, indem Sie die Frage, das Flash-BIOS-Update durchzuführen beantworten.
 - Drücken Sie *n*.
 - Drücken Sie die Eingabetaste.
- ▶ Um das Flash-BIOS-Update für den Prozessor durchzuführen, geben Sie ein:
 - ↳ *bioflash* ↵ /p6
- ▶ Drücken Sie die Eingabetaste.

Flash Memory Recovery Mode



Das BIOS ist im Flash Memory gespeichert. Wenn während des Flash-BIOS-Updates ein Fehler auftritt, ist das *BIOS-Setup* im Flash Memory zerstört. Sie können das *BIOS-Setup* über den *Flash Memory Recovery Mode* wiederherstellen. Wenn dies nicht mehr möglich ist, tauschen Sie das Flash Memory aus oder wenden Sie sich an unseren Service.

- ▶ Schalten Sie das Gerät aus und ziehen Sie den Netzstecker.
- ▶ Öffnen Sie das Gehäuse und schalten Sie mit dem Schalter/Jumper den *Recovery-Modus* (RCV) ein (siehe Handbuch zum Mainboard oder das entsprechende Handbuch im PDF-Format auf der CD "Drivers & Utilities").



Normalerweise sind im Recovery-Modus keine Bildschirmausgaben möglich. Achten Sie auf die Lautsprechertöne.

Das Wiederherstellen des Systems war erfolgreich, wenn Sie die Tonfolge "kurz-kurz-lang-lang-lang" hören und die Diskettenzugriffskontrolle erloschen ist. Das Recovery-Update kann einige Minuten dauern.



Nur dann, wenn eine separate VGA-Baugruppe gesteckt ist, können Sie am Bildschirm den Recovery-Update verfolgen.

Bei einigen Systemen müssen Sie zusätzlich den Schalter "Skip" (SKP) einschalten, um die Ausgaben am Bildschirm zu sehen (siehe Handbuch zum Mainboard oder das entsprechende Handbuch im PDF-Format auf der CD "Drivers & Utilities").

- ▶ Starten Sie das System mit eingelegter Flash-BIOS-Diskette.
- ↳ Dann erscheint die Meldung:
RECOVERY MODE
- ▶ Schalten Sie das Gerät aus und ziehen Sie den Netzstecker.
- ▶ Entfernen Sie die Diskette aus Laufwerk A:.
- ▶ Stellen Sie alle Schalter, die Sie geändert haben (z. B. "RCV/SKP"), in die Ausgangsposition zurück.
- ▶ Schalten Sie das Gerät wieder ein.
- ↳ Der PC fährt mit der neuen BIOS-Version hoch.
- ▶ Prüfen Sie die Einstellungen im *BIOS-Setup*. Konfigurieren Sie diese gegebenenfalls neu.

DeskFlash



Ein Flash-BIOS-Update kann bei einigen Mainboards direkt unter Windows durchgeführt werden mit dem Utility *DeskFlash*, das sich auf der CD "Drivers & Utilities" befindet.

In der Datei *Liesmich* oder *Readme* im Unterverzeichnis *DeskFlash* finden Sie die Installationsanleitung für *DeskFlash*.

Weitere Informationen zu *DeskFlash* finden Sie in der Datei *\\...\\DeskView.PDF* und in der Online-Hilfe von *DeskView*.

TPM (Trusted Platform Module) Configuration

ruft das Untermenü auf indem Sie das TPM aktivieren und Einstellungen vornehmen können.

Mainboards mit diesem Setup Menu enthalten einen Sicherheits- und Verschlüsselungsbaustein (TPM – Trusted Platform Module) gemäß der TCG Spezifikation 1.2.

Ähnlich wie bei SmartCards, können in diesem Baustein sicherheitsrelevante Daten (Passwörter etc.) zugriffssicher abgelegt werden. Die Benutzung des TPM ist standardisiert und von der Trusted Computing Group (TCG) spezifiziert.

TPM Support

aktiviert/deaktiviert die Unterstützung des Trusted Platform Moduls.

Enabled Die Trusted Platform Unterstützung ist aktiviert.

Disabled Die Trusted Platform Unterstützung ist deaktiviert.

TPM State

legt fest, ob das Trusted Platform Modul benutzt werden kann (*Enabled*) oder abgeschaltet ist (*Disabled*). Das Trusted Platform Modul steht als sicherer Speicher für geheime Schlüssel zur Verfügung. Es können z. B. Daten erzeugt werden, die nur auf diesem System lesbar oder ablauffähig sind. Ebenfalls möglich ist die Unterstützung von Sicherheitsprotokollen, wie z.B. SSL (Secure Socket Layer) für Internetverbindungen, IPSec (LAN-Verschlüsselung), S-MIME (E-Mail-Verschlüsselung, WLAN-Verschlüsselung).

Enabled Trusted Platform Module Funktion ist aktiviert.

Disabled Trusted Platform Module Funktion ist deaktiviert.

Security ...		
TPM Configuration		Item Specific Help
Current TPM State	Enabled and Activated	Enable Trusted Platform Module support
TPM Support:	[Enabled]	
TPM State:	[No Change]	

TPM Physical Presence operations

Diese Setup-Seite ist nicht über das normale *BIOS-Setup* erreichbar. Sie erscheint automatisch während des *BIOS POST*, wenn eine Konfigurationsänderung am TPM vorgenommen werden soll. Dies kann entweder durch das BIOS-Setup oder über ein Betriebssystem mit TPM-Unterstützung ausgelöst werden. Die Trusted Computing Group (TCG) Sicherheitsbestimmungen schreiben vor, dass Konfigurationsänderungen nochmals persönlich bestätigt werden müssen (Physical Presence Operations).

Physical Presence Operations	
TPM Configuration change was requested to State: Enabled and Activated	Item Specific Help
Note: This action will switch on the TPM	Reject Physical Presence operations and exit
Reject Execute	

Mögliche Meldungen:

- [1] Enable & Activate
- [2] Deactivate & Disable
- [3] Clear

cME Authentication Level

legt fest, mit welcher Sicherheitsstufe FirstWare Applikationen laufen sollen.

<i>High</i>	hohe Sicherheitsstufe (Standard)
<i>Medium</i>	mittlere Sicherheitsstufe
<i>Low</i>	niedrige Sicherheitsstufe

Virus Warning - Viruswarnung

prüft die Bootsektoren des Festplattenlaufwerks auf Veränderungen gegenüber dem letzten Systemstart. Ist die Ursache der Veränderungen der Bootsektoren unbekannt, dann sollte ein geeignetes Programm zum Auffinden von Computerviren gestartet werden.

<i>Enabled</i>	Wenn sich der Bootsektor seit dem letzten Systemstart verändert hat (z. B. neues Betriebssystem oder Virenbefall), wird eine Warnung am Bildschirm ausgegeben. Die Warnung wird so lange ausgegeben, bis die Änderungen mit <i>Confirm</i> bestätigt werden oder bis Sie die Funktion ausschalten (<i>Disabled</i>).
<i>Confirm</i>	Dieser Eintrag bestätigt eine gewünschte Änderung in einem Bootsektor (z. B. neues Betriebssystem).
Disabled	Die Bootsektoren werden nicht überprüft.

ATA Vulnerability Protection

bietet einen erweiterten Schutz gegen Angriffe auf ATA-Festplatten.

Standard Diese Einstellung betreibt die Festplatte in dem vom Hersteller ausgelieferten Standard. Vor dem Konfigurieren der Festplatte (z.B. Festplattenpasswort, Silent Mode, SMART, ...) sollte die Standardeinstellung gewählt werden.

Enhanced Die Festplatte kann in einen geschützten Modus gebracht werden, in dem deren sicherheitsrelevanten Funktionen nicht mehr identisch mit dem ursprünglich ausgelieferten Zustand sind. Bei dieser Einstellung werden möglicherweise einige spezielle Hardwarenahe Festplatten-Konfigurationsprogramme nicht mehr funktionieren.



Damit eine Änderung der Einstellung wirksam wird, ist gegebenenfalls ein Aus-/Einschalten des Systems nötig.

Diskette Write – Schreibschutz für Diskettenlaufwerk

legt fest, ob Disketten beschrieben und gelöscht werden können.

Enabled Disketten können gelesen, beschrieben oder gelöscht werden, wenn der zugehörige Schalter (siehe Handbuch zum Mainboard) entsprechend eingestellt ist.

Disabled Disketten können nur gelesen werden.

Flash Write – Schreibschutz für System-BIOS

kann das System-BIOS mit einem Schreibschutz versehen.

Enabled Das System-BIOS kann beschrieben oder gelöscht werden, wenn der zugehörige Schalter (siehe Handbuch zum Mainboard) entsprechend eingestellt ist. Ein Flash-BIOS-Update von Diskette ist möglich.

Disabled Das System-BIOS kann nicht beschrieben oder gelöscht werden. Ein Flash-BIOS-Update von Diskette ist nicht möglich.

Cabinet Monitoring – Schutz nach Öffnen des Gehäuses

legt fest, ob nach einem Öffnen des Gehäuses das Gerät weiterarbeitet oder nur nach Eingabe des Setup-Passworts.

Enabled Nach dem Öffnen des Gehäuses können Sie das Gerät nur mit dem Setup-Passwort weiterbetreiben.

Disabled Das Gerät arbeitet auch mit geöffnetem Gehäuse normal weiter. Ein Passwort wird nicht benötigt.

Power Menu – Energiesparfunktionen

Power		
Power-on Source:	[BIOS Controlled]	Item Specific Help
LAN:	[Enabled]	
Wake On LAN boot:	[Boot Sequence]	[BIOS Controlled]
Wake Up Timer:	[Disabled]	Power-on sources
Wake Up Time:	[00.00.00]	are controlled by BIOS
Wake Up Mode:	[Daily]	Also valid for ACPI
		operating systems.
Power Failure Recovery:	[Previous State]	
USB At Power-off:	[Always Off]	[ACPI Controlled]
USB Keyboard	[Disabled]	Power-on source are
		controlled by an ACPI
		operating system.

Beispiel für das Menu *Power*

Power On Source – Verwaltung der Einschaltquellen

legt fest, ob die Einschaltquellen für ACPI-Betriebssysteme vom BIOS oder vom Betriebssystem verwaltet werden.

BIOS Controlled Die Einschaltquellen werden vom BIOS verwaltet.

ACPI Controlled Die Einschaltquellen werden vom ACPI-Betriebssystem verwaltet.

Power On Source: LAN – Einschalten über LAN-Controller

legt fest, ob das System über einen LAN-Controller (auf dem Mainboard oder zusätzliche Baugruppe) eingeschaltet werden kann.

Enabled Das System kann über einen LAN-Controller eingeschaltet werden.

Disabled Das System kann nicht über einen LAN-Controller eingeschaltet werden.

Wake On LAN Boot – Einschalten über Netzwerk

Legt das Verhalten beim Einschalten des Systems über Netzwerksignale fest.

Boot Sequence Nach dem Einschalten über LAN startet das System gemäß der im Boot Menü vorgegebenen Gerätefolge.

Force LAN Boot Nach dem Einschalten über LAN wird über LAN remote gestartet.

Power On Source: Wake Up Timer – Einschalten über Zeit

legt fest, ob das System nach einer festgelegten Einschaltzeit (eine bestimmte Uhrzeit, eine festgelegte Zeitdauer) eingeschaltet werden kann. Das Einschaltdatum kann nicht über das *BIOS-Setup* festgelegt werden. Sie benötigen zur Programmierung des Einschaltdatums ein geeignetes Programm.

- Enabled* Das System kann zeitgesteuert eingeschaltet werden.
Disabled Das System kann nicht zeitgesteuert eingeschaltet werden.



Das Wiedereinschalten nach einem kritischen Systemfehler wird von dieser Einstellung nicht beeinflusst.

Power On Source: Wake Up Time – Einschalten über Zeit

legt den genauen Zeitpunkt fest, zu dem das System eingeschaltet werden soll.

00:00:00

Power On Source: Wake Up Mode

legt die Einschaltperiode fest.

- Daily** Das System wird täglich eingeschaltet.
Monthly Das System wird monatlich eingeschaltet.

Power Failure Recovery – Systemzustand nach einem Stromausfall

legt den Systemzustand nach einem durch Stromausfall bedingten Neustart fest.

- Always Off* Das System schaltet sich kurz ein, prüft seinen aktuellen Zustand (Initialisierung) und schaltet sich wieder ab.
Always On Das System schaltet sich ein.
Previous State Das System schaltet sich kurz ein, prüft seinen aktuellen Zustand und kehrt in den Zustand zurück, in dem es sich vor dem Stromausfall befand (ON oder OFF).
Disabled Das System schaltet sich nicht ein.



In der kurzen Initialisierung werden alle WakeUp-Quellen wieder konfiguriert. Das System kann über über LAN etc. wieder geweckt werden. Bei *Disabled* kann das System nur über die Einschalttaste geweckt werden.

USB At Power-off

aktiviert/deaktiviert die Stromversorgung an den USB-Schnittstellen.

Always off die USB-Schnittstellen werden mit dem Ausschalten des PC stromlos.

Always on die USB-Schnittstellen bleiben auch bei ausgeschaltetem PC unter Strom.

USB Keyboard

aktiviert/deaktiviert den Ein-/Ausschalter der USB-Tastatur.

Enabled Der PC kann über den Ein-/Ausschalter der USB-Tastatur ein/ausgeschaltet werden.

Disabled Der Ein-/Ausschalter der USB-Tastatur ist deaktiviert.

Boot Menu – Systemstart

Boot	
Boot priority order: 1: IDE CD: Type xxxx-(SM) 2: Legacy Floppy Drives 3: IDE 4: Type xxxx-(PM) 4: PCI BEV: BootManage PXE, Slot 00A0 5: 6: 7: 8: Excluded from boot order: : Legacy Network Card : Bootable Add-in Cards	Item Specific Help Keys used to view or configure devices: Up and Down arrows select a device. <+> and <-> moves the device up or down. <f> and <r> specifies the device fixed or removable. <x> exclude or include the device to boot. <Shift + l> enabled or disabled a device. <1 - 4> loads default boot sequence.

hier kann die Reihenfolge der Laufwerke, von denen gebootet werden soll, festgelegt werden.

Bis zu acht Laufwerke (auch z. B. USB-Schnittstellen) können hier gelistet sein.

Boot Priority Order

zeigt die tatsächliche Boot Order an.

- ▶ Wählen Sie mit den Auf- und Ab-Pfeiltasten ein entsprechendes Gerät, um die Reihenfolge der Boot Order zu ändern.
Um die Priorität des ausgewählten Geräts zu ändern, verwenden Sie die **[+]**-Taste für eine höhere und die **[-]**-Taste für eine niedrigere Priorität.
- ▶ Drücken Sie **[x]**, um das ausgewählte Gerät aus der Boot Order zu entfernen.
Das aus der Boot Order entfernte Gerät, wird *Excluded from Boot Order* hinzugefügt.
- ▶ Wählen Sie mit den Tasten **[1]** bis **[4]** eine der 4 möglichen Standard Boot Order Einstellungen.

Excluded from Boot Order

zeigt an, welche Geräte von der Boot Order ausgeschlossen sind.

Geräte, die hier aufgelistet sind, können nicht zum Booten verwendet werden.

- ▶ Wählen Sie mit Hilfe der Cursor-Tasten **↑** oder **↓** ein Gerät aus.
- ▶ Drücken Sie **[x]**, um das Gerät als letzten Eintrag wieder zur *Boot Order Priority* hinzuzufügen.

Exit Menu – BIOS-Setup beenden

Exit	
Save Changes & Exit	Item Specific Help
Discard Changes & Exit	
Get Default Values	Exit System Setup and
Load Previous Values	save your changes to CMOS

Im Menü *Exit* können Sie Einstellungen speichern und das *BIOS-Setup* beenden.

Save Changes & Exit – Speichern und beenden

Um die aktuellen Einträge in den Menüs zu speichern und das *BIOS-Setup* zu beenden, wählen Sie *Save Changes & Exit* und *Yes*. Das Gerät startet neu und die neuen Einstellungen sind wirksam.

Discard Changes & Exit – Beenden ohne speichern

Um die Änderungen zu verwerfen, wählen Sie *Discard Changes & Exit* und *Yes*. Die beim Aufruf des *BIOS-Setup* gültigen Einstellungen bleiben wirksam. Das *BIOS-Setup* wird beendet und das Gerät startet neu.

Get Default Values – Standardeinträge

Um die Standardeinträge für alle Menüs des *BIOS-Setup* zu übernehmen, wählen Sie *Get Default Values* und *Yes*.

Wenn Sie das *BIOS-Setup* mit diesen Einstellungen beenden wollen, wählen Sie *Save Changes & Exit* und *Yes*.

Load Previous Values – Vorhergehende Einträge

Um für alle Menüs die Einträge zu laden, die beim Aufruf des *BIOS-Setup* gültig waren, wählen Sie *Load Previous Values* und *Yes*. Wenn Sie das *BIOS-Setup* mit diesen Einstellungen beenden wollen, wählen Sie *Save Changes & Exit* und *Yes*.

Stichwörter

A

Advanced Menü 14

B

Basis-I/O-Adresse
parallele Schnittstelle 15
Benutzergruppe
installieren 29
Betriebssystem laden, LAN 18
BIOS-Setup 3
aufrufen 3
bedienen 5–6
beenden 48
Sicherheitsfunktionen 22
Systemeinstellungen 14
Systemkonfiguration 7
BIOS-Update
siehe Flash-BIOS-Update 37
BIOS-Version 5, 39
Boot Menü 4
Bootsektor 42

C

Computerviren 42
Controller 14

D

Datum 7
DeskFlash 40
Discard Changes & Exit 48
Diskettenlaufwerk
Schreibschutz 43
Typ 7

E

Erweiterungsspeicher, Größe anzeigen 13
Exit Menü 48

F

F1, Funktionstaste 5
F10, Funktionstaste 31
F12, Funktionstaste 4
F2, Funktionstaste 36
F3, Funktionstaste 36
F5, Funktionstaste 31–32
F6, Funktionstaste 31–32
F7, Funktionstaste 31

F8, Funktionstaste 31–32
F9, Funktionstaste 31–32
Fehlermeldungen 37
Mainboard 37
Festplatte
Übertragungsgeschwindigkeit 10
Festplattenkapazität 9
Festplattenparameter 9
Flash Memory Recovery Mode 40
Flash-BIOS-Diskette 37
Flash-BIOS-Update 37, 43
Fehlermeldung 39
Internet-Adresse 37

G

Get Default Values 48

H

Hochlaufroutine 12–13

I

Installieren von SystemLock 28

L

Lärm, optisches Laufwerk 11
Load Previous Values 48
Lüfterdrehzahl 20

M

Main Menü 7

O

Optisches Laufwerk 11

P

Passwort
Setup-Passwort 22, 24
System-Passwort 22, 24
Passwort Status 12
Performance, erhöhen 10
Peripherie 14
Pin, ändern 36

R

Recovery Mode 40

- S**
- Save Changes & Exit 48
 - Schnittstelle 14
 - Schreibschutz
 - Diskettenlaufwerk 43
 - System-BIOS 43
 - Security Menü 22
 - Selbsttest 13
 - Setup,
 - siehe BIOS-Setup 3
 - Setup-Passwort 22, 24
 - SmartCard 26
 - Benutzergruppen 27
 - Pin 27
 - Puk 27
 - Zugriffsrechte 27
 - SmartCard-Leser 37
 - Speicher
 - Arbeitsspeicher 13
 - Erweiterungsspeicher 13
 - Hauptspeicher 13
 - Stromausfall, Verhalten des Systems 45
 - System einschalten 26
 - LAN-Controller 44
 - Netzwerk 44
 - zeitgesteuert 45
 - System-BIOS, Schreibschutz 43
 - System-Passwort 22, 24
 - deaktivieren 25
 - eingeben 25
 - Systemeinstellungen, zusätzliche 19
 - SystemLock
 - einschalten 36
 - SystemLock 2
 - installieren 31
 - Systemstart 12–13
 - fehlerhaft 4
- T**
- Tastatur
 - Ein-/Ausschalter 46
- U**
- Uhrzeit 7
 - Update
 - siehe Flash-BIOS-Update 37
 - USB-Controller 17
 - USB-Tastatur-Emulation 17
- V**
- Viruswarnung 42
- W**
- Wake On LAN, System-Passwort 25
 - Wake Up Mode 45
 - Wake Up Time 45